# Vrai-Faux

**1.** **(a)** *L'assertion est fausse.*
On choisit $p = 2$ qui est un nombre premier et $n = 2$ ; on se place dans $\mathbf{Z}/4\mathbf{Z}$. Si la classe de 2 est inversible, il existe un entier $k$ tel que $\overline{2k} = \overline{1}$. En multipliant par $\overline{2}$, on obtient $\overline{0} = \overline{2}$. Cette égalité est fausse donc la classe de 2 n'est pas inversible. Puisque $\overline{2} \neq \overline{0}$, on en déduit que $\mathbf{Z}/4\mathbf{Z}$ n'est pas un corps.

**(b)** *L'assertion est fausse.*
On choisit $p = 7$. Les inversibles de $\mathbf{Z}/7\mathbf{Z}$ sont donnés par les classes des entiers premiers avec 7, l'ensemble $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ est le sous-groupe multiplicatif des éléments inversibles de $\mathbf{Z}/7\mathbf{Z}$. Par ailleurs, le sous-groupe engendré par $\overline{2}$ est $\{\overline{2}; \overline{4}; \overline{1}\}$, on en conclut que $\overline{2}$ n'engendre pas le groupe des inversibles de $\mathbf{Z}/7\mathbf{Z}$.

**(c)** *L'assertion est vraie.*
Les éléments inversibles de $\mathbf{Z}/9\mathbf{Z}$ sont les classes des entiers $k$ entre 1 et 8 tels que $\mathrm{pgcd}(k, 9) = 1$, ce sont les classes de $1, 2, 4, 5, 7, 8$. Les puissances de $\overline{2}$ sont les classes de 2, 4, 8, 7, 5 et 1 donc $\overline{2}$ engendre le sous-groupe multiplicatif des éléments inversibles de $(\mathbf{Z}/9\mathbf{Z})$.

**(d)** *L'assertion est fausse.*
Pour $a = 1$, $b = -1$, $c = 1$, $d = 4$, on a $M = \begin{pmatrix} 1 & -1 \\ 1 & 4 \end{pmatrix}$ et $\det(M) = 5$ donc $M$ est inversible. En revanche, on a $\det(\overline{M}) = \overline{5} = \overline{0}$ donc la matrice $\overline{M}$ n'est pas inversible dans $\mathcal{M}_2(\mathbf{Z}_{/5\mathbf{Z}})$.

**(e)** *L'assertion est vraie.*
Soit $\mu : K \mapsto L$ un morphisme de corps. Si $x$ est un élément non nul de $K$, il est inversible et $xx^{-1} = 1_K$. Puisque $\mu$ est un morphisme, $\mu(x)\mu(x^{-1}) = \mu(1_k) = 1_L$. On en déduit que $\mu(x)$ n'est pas nul donc $x$ ne peut pas être dans le noyau du morphisme $\mu$. Le noyau de $\mu$ est donc $\{0_K\}$ et $\mu$ est injectif.

# Exercice 1

**2.** - On suppose que $x_{k+1} \in \mathrm{Vect}(x_1, \cdots, x_k)$, ainsi il existe des scalaires $(\alpha_1, \ldots, \alpha_k) \in \mathbb{K}^k$ tels que

$$x_{k+1} = \sum_{i=1}^{k} \alpha_i x_i.$$

On a alors $\alpha_1 x_1 + \cdots + \alpha_k x_k - x_{k+1} = 0$ avec $(\alpha_1, \ldots, \alpha_k, -1) \neq (0, \ldots, 0)$ donc la famille $(x_1, \ldots, x_{k+1})$ est liée.

- Réciproquement, supposons que la famille $(x_1, \ldots, x_{k+1})$ soit liée, il existe alors des scalaires $\beta_1, \ldots, \beta_k, \beta_{k+1}$ non tous nuls tels que $\displaystyle\sum_{i=1}^{k+1} \beta_i x_i = 0$. Si $\beta_{k+1}$ est nul, alors $\displaystyle\sum_{i=1}^{k} \beta_i x_i = 0$ ; or la famille $(x_1, \ldots, x_k)$ est libre, on en déduit que tous les $\beta_i$ sont nuls ce qui est absurde. Puisque $\beta_{k+1}$ est non nul et on peut écrire $x_{k+1} = \displaystyle\sum_{i=1}^{k} \alpha_i x_i$ avec $\alpha_i = -\dfrac{\beta_i}{\beta_{k+1}}$ donc $x_{k+1}$ est combinaison linéaire de $(x_1, \ldots, x_k)$.

L'équivalence demandée est alors démontrée.

**3.** On fixe $n \in \mathbf{N}^*$ et on raisonne par récurrence finie sur $k \leqslant n$.
Pour $k = 1$ : une famille de un seul vecteur est libre si et seulement si ce vecteur est non nul. Il y

a $p^n$ vecteurs dans $\mathbb{K}^n$ donc $p^n - 1$ vecteurs non nuls.
Soit $k \in [\![1; n-1]\!]$. On suppose que le nombre de familles libres de $k$ vecteurs est $(p^n - 1)(p^n - p)\cdots(p^n - p^{k-1})$. D'après la question précédente, les familles libres de $k+1$ vecteurs sont composées d'une famille libre de $k$ vecteurs et d'un vecteur qui n'est pas combinaison linéaire des $k$ premiers.
Si $(x_1, \ldots, x_k)$ sont $k$ vecteurs formant une famille libre, alors l'application $(\lambda_1, \ldots, \lambda_k) \mapsto \sum_{i=1}^{k} \lambda_i x_i$ est une bijection de $\mathbb{K}^k$ dans $\mathrm{Vect}(x_1, \ldots, x_k)$. Par conséquent, il y a $p^k$ combinaisons linéaires possibles avec les vecteurs de la famille $(x_1, \ldots, x_k)$ ; on en déduit qu'il y a $p^n - p^k$ choix possibles pour le vecteur $x_{k+1}$. Le nombre de familles libres de $k+1$ vecteurs de $\mathbb{K}^n$ est donc $(p^n - 1)(p^n - p)\cdots(p^n - p^{k-1})(p^n - p^k)$.
La propriété est héréditaire, par récurrence finie, on conclut alors que le résultat est vrai pour tout entier $k$ entre 1 et $n$.

**4.** Une matrice $M \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si ses colonnes forment une famille libre de $\mathcal{M}_{n,1}(\mathbb{K})$ que l'on peut identifier à $\mathbb{K}^n$ donc le cardinal de $GL_n(\mathbb{K})$ est $(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})$.

# Exercice 2

**5. (a)** Soient $i \in \mathbf{N}^*$ et $a \in [\![0; p^i - 1]\!]$. L'entier $a$ n'est pas premier avec $p^i$ si et seulement si $p$ divise $a$ donc si et seulement si $a$ est de la forme $pb$ avec $b \in [\![0; p^{i-1} - 1]\!]$. Il y a donc $p^{i-1}$ entiers non premiers avec $p^i$. Par conséquent, $\varphi(p^i) = p^i - p^{i-1}$.
Soit $k \in \mathbf{N}^*$. Les diviseurs de $p^k$ sont les $p^i$ pour $i$ allant de 0 à $k$ et $\varphi(1) = 1$ donc

$$f(p^k) = 1 + \sum_{i=1}^{k} (p^i - p^{i-1}) = 1 + p^k - p^0.$$

Finalement, on obtient l'égalité $f(p^k) = p^k$.

**(b)** Soient $(d_1, d_2)$ un couple d'éléments de $\mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$. Si $d_1$ divise $m_1$ et $d_2$ divise $m_2$, alors $d_1 d_2$ divise $m_1 m_2$ donc $d_1 d_2$ est un élément de $\mathcal{D}_{m_1 m_2}$ et $P$ est bien définie.
Soit $d \in \mathcal{D}_{m_1 m_2}$. On décompose $d$ en un produits de facteurs premiers distincts : $d = \prod_{p \in I} p^{\alpha_p}$ où $I$ est une partie finie de l'ensemble des nombres premiers et les $\alpha_p$ des entiers naturels non nuls. Pour tout $p \in I$, $p$ divise $m_1 m_2$ et $p$ est premier donc $p$ divise $m_1$ ou $p$ divise $m_2$ mais $p$ ne peut pas diviser $m_1$ et $m_2$. On peut donc écrire $I = I_1 \cup I_2$ où $I_k$ est l'ensemble des $p \in I$ tels que $p$ divise $m_k$. Par conséquent, si on pose $d_k = \prod_{p \in I_k} p^{\alpha_p}$, on a $d = f(d_1, d_2)$. Ceci nous permet de conclure que $f$ est surjective.
Par ailleurs, considérons $((d_1, d_2), (d_1', d_2')) \in (\mathcal{D}_{m_1} \times \mathcal{D}_{m_2})^2$ tel que $d_1 d_2 = d_1' d_2'$. Comme $d_1$ divise $m_1$ qui est premier avec $m_2$ et $d_2'$ divise $m_2$, $d_1$ est premier avec $d_2'$. D'après le théorème de Gauss, $d_1$ divise $d_1'$. De même $d_1'$ divise $d_1$ donc $d_1 = d_1'$ (on ne s'intéresse aux diviseurs dans $\mathbf{N}$). On obtient alors $d_2 = d_2'$ ce qui permet de conclure que $P$ est injective.
Finalement, on a démontré que $P$ est bijective.

**(c)** Par distributivité,

$$f(m_1)f(m_2) = \sum_{(d_1,d_2) \in \mathcal{D}_1 \times \mathcal{D}_2} \varphi(d_1)\varphi(d_2)$$

Comme on l'a vu ci-dessus, si $(d_1, d_2) \in \mathcal{D}_1 \times \mathcal{D}_2$, alors $d_1$ et $d_2$ sont premiers entre eux donc

$$f(m_1)f(m_2) = \sum_{(d_1,d_2)\in\mathcal{D}_1\times\mathcal{D}_2} \varphi(d_1d_2).$$

En utilisant que $P$ est bijective, on a alors $f(m_1)f(m_2) = f(m_1m_2)$.

**(d)** Soit $n \in \mathbf{N}^*$. Si $n = 1$, la relation est vraie. Sinon, on écrit la décomposition de $n$ en facteurs premiers distincts : $n = \prod_{p\in I} p^{\alpha_p}$.

Montrons alors par récurrence sur le cardinal de $I$ que l'on a $f(n) = \prod_{p\in I} f(p^{\alpha_p})$.

— Si $I$ est de cardinal 1, alors $f(n) = f(p^{\alpha_p})$.

— Supposons qu'il existe un entier $k$ tel que si $I$ est de cardinal $k \geqslant 1$ alors

$$(HR)\quad f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_{p_i}}).$$

Soit $n'$ un entier dont la décomposition en facteur premiers comporte $k+1$ nombre premier distincts $p_1, \ldots, p_{k+1}$. Puisque $p_{k+1}$ est premier avec tous les $p_i$, où $i = 1, \ldots, k$, il est aussi premier avec $\prod_{i=1}^{k} p_i$ ; d'après la question précédente, on en déduit l'égalité $f(n') = f\Big(\prod_{i=1}^{k} p_i^{\alpha_{p_{k+1}}}\Big) f(p_{k+1}^{\alpha_{p_{k+1}}})$. En utilisant $(HR)$ on obtient $f(n') = f(p_{k+1}^{\alpha_{p_{k+1}}}) \prod_{i=1}^{k} f(p_i^{\alpha_{p_i}})$. La propriété $(HR)$ est héréditaire et, par récurrence sur le cardinal de $I$, elle est vérifiée pour tout $I$ de cardinal fini.

Étant donné un entier $n = \prod_{p\in I} p^{\alpha_p}$, à l'aide de a question a) on obtient les égalités

$$\sum_{d\in\mathcal{D}_n} \varphi(d) = f(n) = \prod_{p\in I} f(p^{\alpha_p}) \overset{a)}{=} \prod_{p\in I} p^{\alpha_p} = n.$$

**6.** **(a)** Comme $K^*$ est de cardinal $c$, d'après le théorème de Lagrange, l'ordre de tout élément de $K^*$ est un diviseur de $c$ donc $\sum_{d\in\mathcal{D}_c} N(d) = c$.

**(b)** i. Les $d$ éléments de $H$ vérifient $x^d = 1$, ils sont donc racines du polynôme $X^d - 1$. Ce polynôme de degré $d$ a au plus $d$ racines, par conséquent, tout élément de $K^*$ d'ordre $d$ est dans $H$ et est un générateur de $H$.

ii. Soit $d$ diviseur de $c$. Si dans $K^*$ il n'existe pas d'élément d'ordre $d$, alors $N(d) = 0 \leqslant \varphi(d)$. S'il en existe un, que l'on note $x$, alors d'après la question précédente on sait que tout élément d'ordre $d$ est un générateur du sous-groupe $H$ engendré par $x$. Puisque $H$ est cyclique, il est isomorphe à $\mathbf{Z}/d\mathbf{Z}$ donc il admet $\varphi(d)$ générateurs. Dans ce cas, on a $N(d) \leqslant \varphi(d)$.

L'inégalité est donc toujours vraie.

**(c)** Les question 5.d) et 6.a) permettent d'écrire $\sum_{d\in\mathcal{D}_c} (\varphi(d) - N(d)) = 0$. D'après la question précédente, il s'agit d'une somme de réels positifs. Par conséquent, chaque membre de cette somme est nul et, pour tout $d \in \mathcal{D}_c$, on a $N(d) = \varphi(d)$. En particulier $N(c)$ n'est pas nul et $K^*$ admet un élément d'ordre $c$. Comme il est de cardinal $c$, cela signifie que $K^*$ est cyclique.

# Problème

## Partie I : Valuation et valeur absolue $p$-adiques

### I.A Définition de la valuation

**7.** Soit $n \in \mathbf{Z}^*$ et soit $A = \{i \in \mathbf{N} \ / \ p^i \text{ divise } n\}$. Puisque 0 est élément de $A$, cet ensemble est non vide. De plus, si $i \geqslant |n|$, alors on a $p^i \geqslant 2^{|n|} \geqslant |n|$ ; ainsi, le sous-ensemble $A$ de $\mathbf{N}$ est majorée par $|n|$. On en déduit que $A$ admet un plus grand élément que l'on note $k$. Par définition, $p^k$ divise $n$ et $p^{k+1}$ ne divise pas $n$. Soit $l$ un entier naturel vérifiant $p^l$ divise $n$ et $p^{l+1}$ ne divise pas $n$. Si $l < k$, alors $p^{l+1}$ divise $p^k$ donc $p^{l+1}$ divise $n$ ce qui n'est pas possible. De même, on ne peut pas avoir $k < l$. On en déduit que $l = n$ ; par conséquent, il existe un unique entier naturel $k$ tel que $p^k$ divise $n$ et $p^{k+1}$ ne divise pas $n$.

**8.** Soit $(a, b) \in (\mathbf{Z}^*)^2$. Posons $k = v_p(a)$ et $l = v_p(b)$. On peut alors écrire $a = p^k a'$ avec $a'$ qui est premier avec $p$. De même, on pose $b = p^l b'$ avec $b'$ premier avec $p$. Ainsi $ab = p^{k+l} a'b'$ où, comme $a'$ et $b'$ sont premiers avec $p$, l'entier $a'b'$ est premier avec $p$. On en déduit que $p^{k+l}$ divise $ab$ et $p^{k+l+1}$ ne divise pas $ab$ ce qui se traduit par $v_p(ab) = k + l = v_p(a) + v_p(b)$.

**9.** Soit $(a, b, c, d) \in (\mathbf{Z}^*)^4$ tel que $\dfrac{a}{b} = \dfrac{c}{d}$. D'après la question précédente, l'égalité $ad = bc$ implique $v_p(a) + v_p(d) = v_p(b) + v_p(c)$ ; on en déduit que $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

**10.** Soit $(r, s) \in (\mathbf{Q}^*)^2$, posons $r = \dfrac{a}{b}$ et $s = \dfrac{c}{d}$. Alors $rs = \dfrac{ac}{bd}$ et

$$v_p(rs) = v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - v_p(b) - v_p(d),$$

donc

$$v_p(rs) = (v_p(a) - v_p(b)) + (v_p(c) - v_p(d)) = v_p(r) + v_p(s).$$

**11.** Soit $(r, s) \in (\mathbf{Q}^*)^2$ tel que $r \neq s$. Dans un premier temps, on suppose que $r$ et $s$ sont des entiers relatifs. Posons $k = v_p(r)$ et $l = v_p(s)$, on peut alors écrire $r = p^k r'$ et $s = p^l s'$ où $r'$ et $s'$ sont des entiers premiers avec $p$. On en déduit que, si $m = \min(k, l)$, alors $p^m$ divise $r - s$ ce qui implique $v_p(r - s) \geqslant m$. Pour $r$ et $s$ rationnels quelconques (avec toujours $r \neq s$), on note $r = \dfrac{a}{b}$ et $s = \dfrac{c}{d}$. Alors $r - s = \dfrac{ad - bc}{bd}$ et $v_p(r - s) = v_p(ad - bc) - v_p(bd)$. En utilisant le premier cas et ce qui précède,

$$v_p(r - s) \geqslant \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d).$$

Si l'on suppose $v_p(ad) \leqslant v_p(bc)$, alors $v_p(r) \leqslant v_p(s)$ et $v_p(r - s) \geqslant v_p(ad) - v_p(b) - v_p(d)$ donc $v_p(r - s) \geqslant v_p(r)$. Si $v_p(ad) > v_p(bc)$, alors $v_p(r) > v_p(s)$ et $v_p(r - s) \geqslant v_p(bc) - v_p(b) - v_p(d)$ donc $v_p(r - s) \geqslant v_p(s)$.

Dans tous les cas, nous avons $v_p(r - s) \geqslant \min(v_p(r), v_p(s))$.

**12.** Si $r = 0$, alors $rs = 0$ et pour avoir la relation de la question **10.**, il suffit de considérer que, pour tout entier $k$, on a $+\infty + k = +\infty$.

Pour la question **11.**, si $s = 0$, alors $r - s = r$ et on convient que $\min(+\infty, k) = k$ pour tout $k \in \mathbf{Z}$.

Si $r = 0$, alors $r - s = -s$ et $v_p(-s) = v_p(s)$.

# I.B Etude de $v_p(n!)$

**13.** Soit $k \in \mathbf{N}$. Pour $i$ entre 1 et $n$, on a $v_p(i) \geqslant k$ si et seulement si $p^k$ divise $i$. Le nombre d'entiers $i$ entre 1 et $n$ tels que $v_p(i) \geqslant k$ est donc le nombre de multiples de $p^k$ entre 1 et $n$. Ces multiples sont de la forme $p^k m$ avec $m \in \mathbf{N}$ tel que $1 \leqslant p^k m \leqslant n$ c'est-à-dire $1 \leqslant m \leqslant \dfrac{n}{p^k}$.

Par conséquent, le nombre d'entiers $i$ entre 1 et $n$ tels que $v_p(i) \geqslant k$ est $\left\lfloor \dfrac{n}{p^k} \right\rfloor$. On le note $n_k$.

**14.** On note $a_k$ le nombre d'entiers $i$ entre 1 et $n$ tels que $v_p(i) = k$, c'est-à-dire tel que $v_p(i) \geqslant k$ sans que $v_p(i)$ soit supérieur ou égal à $k+1$. On a donc $a_k = n_k - n_{k+1}$ et d'après la question **8.** on sait que $v_p(n!) = \sum_{i=1}^{n} v_p(i)$. En regroupant dans cette somme les termes selon la valeur de $v_p(i)$, on obtient

$$v_p(n!) = \sum_{k=0}^{+\infty} k a_k$$

qui est un somme finie car $a_k$ est nul pour $k$ assez grand. Par ailleurs, on a $a_k = n_k - n_{k+1}$ et du fait que les sommes n'ont qu'un nombre fini de termes non nuls on en déduit que

$$v_p(n!) = \sum_{k=0}^{+\infty} k n_k - \sum_{k=1}^{+\infty} (k-1) n_k = 0 + \sum_{k=1}^{+\infty} (k - (k-1)) n_k.$$

Ainsi,

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

**15.** En écrivant la décomposition en facteurs premiers de 100!, on constate que le nombre de zéros à la fin de 100! correspond à $\min(v_2(100!), v_5(100!))$.

$$v_2(100!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{100}{2^k} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97,$$
$$v_5(100!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{100}{5^k} \right\rfloor = 20 + 4 = 24.$$

Il y a donc 24 zéros à la fin de 100!.

**16.** Soit $n \in \mathbf{N}^*$.

Pour tout $k \geqslant 1$, on a $\left\lfloor \dfrac{n}{p^k} \right\rfloor \leqslant \dfrac{n}{p^k}$ et $\sum_k \dfrac{n}{p^k}$ est une série géométrique convergente donc

$$v_p(n!) \leqslant \sum_{k=1}^{+\infty} \frac{n}{p^k} \leqslant \frac{n}{p} \frac{1}{1 - \frac{1}{p}}$$

donc

$$v_p(n!) \leqslant \frac{n}{p-1}.$$

## I.C Une caractérisation des puissances de 2

**17.** Soit $k \geqslant 1$. On part de la décomposition de $k$ en base 2 de la forme suivante $k = \sum_{i=0}^{q} u_i 2^i$ avec $u_q \neq 0$.
Si, pour tout $i$, $u_i = 1$, alors $k+1 = 2^{q+1}$. On a alors $s(k) = q+1$, $s(k+1) = 1$ et $v(k+1) = q+1$. La relation est vérifiée dans ce cas. Sinon, on peut considérer le plus petit entier $r$ tel que $u_r = 0$. Pour $i < r$, on a $u_i = 1$ et la décomposition de $k+1$ est $k+1 = \sum_{i=0}^{q} u'_i 2^i$ avec $u'_i = 0$ pour $i < r$, $u'_r = 1$ et, pour $i > r$, on a $u'_i = u_i$. On a alors $s(k) - s(k+1) = r - 1$ et $v(k+1) = r$ donc la relation est vraie.

**18.** En utilisant **8.**, $v_2(n!) = \sum_{k=2}^{n} v_2(k)$ et, par télescopage, on a $v_2(n!) = s(1) - s(n) + n - 1$. Comme $s(1) = 1$, on a

$$v_2(n!) = n - s(n).$$

**19.** On suppose que $n = 2^q$ avec $q \in \mathbf{N}^*$.

$$\begin{aligned} v_2\left(\binom{n}{k}\right) &= v_2(n!) - v_2(k!) - v_2((n-k)!) \\ &= n - s(n) - k + s(k) - (n-k) + s(n-k) \\ &= s(k) + s(n-k) - s(n) \\ &= s(k) + s(n-k) - 1. \end{aligned}$$

Comme $k$ et $n-k$ ne sont pas nuls, $s(k) \geqslant 1$ et $s(n-k) \geqslant 1$. On en déduit que $v_2\left(\binom{n}{k}\right) \geqslant 1$ ce qui signifie que 2 divise $\binom{n}{k}$ et donc que $\binom{n}{k}$ est pair.

**20.** On suppose que, pour tout $k \in [\![1; n-1]\!]$, $\binom{n}{k}$ est pair. Si $n$ n'est pas une puissance de 2, alors on pose $k = 2^q$ la plus grande puissance de 2 qui divise $n$ ; on a alors $n = 2^q l$ avec $l$ impair différent de 1. D'après l'hypothèse de départ, on a $\binom{n}{k}$ est pair. De plus, d'après la question précédente nous avons l'égalité $v_2\left(\binom{n}{k}\right) = s(k) + s(n-k) - s(n)$. Comme $n = 2^q l$, on a $s(n) = s(l)$ ; de plus $s(k) = s(2^q) = 1$ et $n - k = 2^q(l-1)$ donc $s(n-k) = s(l-1)$. Ainsi

$$v_2\left(\binom{n}{k}\right) = 1 + s(l-1) - s(l) = v_2(l) = 0,$$

ce qui est absurde. Par conséquent si, pour tout $k \in [\![1; n-1]\!]$, $\binom{n}{k}$ est pair, alors $n$ est une puissance de 2.

## I.D Valeur absolue $p-$adique

**21.** Soit $(x,y) \in \mathbf{Q}^2$. En utilisant la question **10.**, on a $|xy|_p = |x|_p|y|_p$. De même, en utilisant la question **11.** et $p > 1$, on a $|x-y|_p \leqslant \max(|x|_p, |y|_p)$. Comme $|x|_p$ et $|y|_p$ sont positifs, on a

$$|x+y|_p = |x-(-y)|_p \leqslant \max(|x|_p, |y|_p) \leqslant |x|_p + |y|_p.$$

**22.** Soit $(x,y,z) \in \mathbf{Q}^3$.

— On a $d_p(x,z) = |x-z|_p = |x-y+y-z|_p$ donc en utilisant l'inégalité de la question **21.**, on obtient

$$d_p(x,z) \leqslant \max(d_p(x,y), d_p(y,z)).$$

et $d_p$ est une application de $\mathbf{Q}^2$ dans $\mathbf{R}^+$.

— Pour tout $(x,y) \in \mathbf{Q}^2$, on a $d_p(x,y) = d_p(y,x)$.

— Pour tout $(x,y,z) \in \mathbf{Q}^2$, d'après ce qui précède, on a $d_p(x,z) \leqslant d_p(x,y) + d_p(y,z)$.

— Soit $(x,y) \in \mathbf{Q}^2$. Par définition de $|\cdot|$, si $r \in \mathbf{Q}^*$, alors $|r|_p > 0$. Par conséquent, si $d_p(x,y) = 0$, alors $|x-y|_p = 0$ ce qui implique $x-y=0$ et $x=y$. Réciproquement si $x=y$, on a bien $d_p(x,y)=0$.

On peut alors conclure que $d_p$ est une distance sur $\mathbf{Q}$.

**23.** Pour $n \in \mathbf{N}$, on a $v_p(p^n) = n$ donc $|p^n|_p = \dfrac{1}{p^n}$. Par conséquent, on obtient que $\lim\limits_{n\to+\infty} d_p(p^n, 0) = 0$ et la suite $(p^n)_{n\geqslant 0}$ converge vers 0 dans l'espace métrique $(\mathbf{Q}, d_p)$.

# Partie II : Les entiers $p$-adiques

## II.A Définition de $\mathbf{Z}_p$

**24.** Soit $(a_n)_{n\geqslant 0}$ une suite de $\mathbf{N}$ telle que pour tout $n \in \mathbf{N}$, on a $a_n \in [\![0; p^{n+1}-1]\!]$. Si, pour tout couple $(n,m)$ de $\mathbf{N}^2$ tel que $m \geqslant n$, on a $a_m \equiv a_n[p^{n+1}]$ ; alors on en déduit que $a_{n+1} \equiv a_n[p^{n+1}]$.
Réciproquement, supposons que, pour tout $n \in \mathbf{N}$, on a $a_{n+1} \equiv a_n[p^{n+1}]$. On fixe $n \in \mathbf{N}$, en remarquant que, si $x \equiv y[p^k]$, alors pour $l \leqslant k$, $x \equiv y[p^l]$ ; on démontre par récurrence sur $m \geqslant n$ que $a_m \equiv a_n[p^{n+1}]$.
On peut alors conclure que l'équivalence proposée est vraie.

**25.** On a $a_n \equiv a_{n+1}[p^{n+1}]$ et $a_{n+1} = \sum_{i=0}^{n} u_i p^i + u_{n+1}p^{n+1}$ donc $a_n \equiv \sum_{i=1}^{n} u_i p^i[p^{n+1}]$. De plus, puisque $a_n \leqslant p^{n+1}-1$ et $\sum_{i=0}^{n} u_i p^i \leqslant \sum_{i=0}^{n}(p-1)p^i \leqslant p^{n+1}-1$ on en déduit que $a_n = \sum_{i=0}^{n} u_i p^i$ qui est la décomposition de $a_n$ en base $p$.

**26.** Soit $a$ non nul dans $\mathbf{Z}_p$ et $u$ comme dans la question précédente. Si $u$ est la suite nulle, alors pour tout $n$, on a $a_n = 0$ ce qui est exclu. On peut donc considérer l'unique entier $k = \min\{l \in \mathbf{N} \ / \ u_l \neq 0\}$.

— Si $n < k$, on a $a_n = 0$ et $v_p(a_n) = +\infty$.

— Si $n = k$, on a $a_n = u_k p^k$ avec $u_k$ non divisible par $p$ donc $v_p(a_n) = k$.

— Si $n > k$, $a_n = u_k p^k + cp^{k+1}$ avec $c$ entier et $u_k$ non divisible par $p$ donc $v_p(a_n) = k$.

**27.** Par construction, pour tout $n \in \mathbf{N}$, on a $a_n \in [\![0; p^{n+1}-1]\!]$. De plus, $a_{n+1} \equiv x[p^{n+2}]$ donc $a_{n+1} \equiv x[p^{n+1}]$ et $a_{n+1} \equiv a_n[p^{n+1}]$. La question **24.** permet alors de conclure que $a \in \mathbf{Z}_p$.

**28.** Pour $x = 7$, $a_0 = 2$ (reste de 7 modulo 5) et, pour $n \geqslant 1$, on a $a_n = 7$. Pour $x = -7$, $a_0 = 3$ et, pour $n \geqslant 1$, on a $a_n = p^{n+1} - 7$ (puisque $-7 = (-1)p^{n+1} + (p^{n+1} - 7)$ avec $p^{n+1} - 7 < p^{n+1}$.

**29.** Soient $x$ et $x'$ deux entiers relatifs tels que $\theta(x) = \theta(x')$. Considérerons un entier $n_0$ tel que

$|x| < p^{n_0+1}$ et $|x'| < p^{n_0+1}$.

— Si $x$ et $x'$ sont positifs, pour $n \geqslant n_0$, on a $\theta(x)_n = x$ et $\theta(x')_n = x'$ donc $x = x'$.

— Si $x$ est positif et $x'$ est strictement négatif, on a $\theta(x)_n = x$ et $\theta(x')_n = p^{n+1} - x'$ donc $x = p^{n+1} - x'$, ce qui est impossible car cela devrait être vrai pour tout $n \geqslant n_0$.

— On traite de la même manière les deux derniers cas.

On peut alors conclure que $\theta$ est une application injective.

**30.** Soient $n \in \mathbf{N}$ et $p$ un nombre premier impair. On a $a_n \geqslant 0$ et $a_n = \dfrac{p^{n+1}-1}{p-1}$ avec $p - 1 \geqslant 1$ donc $a_n \leqslant p^{n+1} - 1$. De plus $a_{n+1} = a_n + p^{n+1}$ donc $a_{n+1} \equiv a_n[p^{n+1}]$, par conséquent $a \in \mathbf{Z}_p$. Supposons qu'il existe $x \in \mathbf{Z}$ tel que $a = \theta(x)$. Pour $n$ assez grand, on a $a_n = x$ ou $x = a_n - p^{n+1}$. Le premier cas est impossible et dans le second cas, l'égalité $x = \dfrac{p^{n+1}-1}{p-1} - p^{n+1}$, est également impossible. Il n'existe donc pas de $x \in \mathbf{Z}$ tel que $\theta(x) = a$.

**31.** — Si $x = 0$, on a $\theta(x) = 0$ et $\tilde{v}_p(\theta(x)) = v_p(x)$.

— Si $x$ n'est pas nul, on pose $a = \theta(x)$.

  — Si $x$ est positif, on a $a_n = x$ pour $n$ assez grand donc $v_p(a_n) = v_p(x)$.

  — Si $x$ est négatif, on a $a_n = p^{n+1} - x$ pour $n$ assez grand et pour $n \geqslant v_p(x)$, on obtient $v_p(a_n) = v_p(x)$.

Dans tous les cas, on a $\tilde{v}_p(\theta(x)) = v_p(x)$.

## II.B. Structure d'anneau

**32.** Par définition, pour tout $n \in \mathbf{N}$, $c_n \in [\![0; p^{n+1} - 1]\!]$ et par compatibilité de l'addition par rapport à la congruence, pour $n \in \mathbf{N}$, on a $c_{n+1} \equiv c_n[p^{n+1}]$. On en déduit que $c \in \mathbf{Z}_p$.

**33.** Il est immédiat que la suite nulle est un élément neutre. On vient de vérifier que + est une loi de composition interne dans $\mathbf{Z}_p$ qui est commutative. Soient $a$, $b$ et $c$ trois éléments de $\mathbf{Z}_p$. On pose $d = a + b$, $e = d + c = (a + b) + c$, $f = (b + c)$ et $g = a + f$. Pour vérifier l'associativité de la loi +, il faut montrer que $e = g$.

Pour $n \in \mathbf{N}$, on a $d_n \equiv a_n + b_n[p^{n+1}]$ et $e_n \equiv d_n + c_n[p^{n+1}]$ donc $e_n \equiv a_n + b_n + c_n[p^{n+1}]$ (on utilise l'associativité de l'addition dans $\mathbf{Z}$). On procède de même avec $g_n$ et on obtient $e_n \equiv g_n[p^{n+1}]$. Comme $e_n$ et $g_n$ sont des entiers compris entre 0 et $p^{n+1} - 1$, cela permet de conclure que $e = g$ et la loi + est associative dans $\mathbf{Z}_p$.

Soit $a \in \mathbf{Z}_p$. On définit l'élément $b$ de $\mathbf{Z}_p$ en posant $b_n = 0$ si $a_n = 0$ et $b_n = p^{n+1} - a_n$ si $a_n \neq 0$. Pour tout entier $n$, l'entier $b_n$ est entre 0 et $p^{n+1} - 1$ et $b_n \equiv -a_n[p^{n+1}]$ ; on en déduit que $a_n + b_n \equiv 0[p^{n+1}]$. On peut alors conclure que $(\mathbf{Z}_p, +)$ est un groupe commutatif ; l'élément neutre étant la suite nulle.

**34.** Soit $e \in \mathbf{Z}_p$ tel que, pour tout $n$, $e_n = 1$ ($e = \theta(1)$). Alors l'élément $e$ est le neutre de la multiplication.

**35.** Soient $a$ et $b$ deux éléments non nuls de $\mathbf{Z}_p$. Pour un entier $n$ assez grand, les entiers $a_n$ et $b_n$ sont non nuls et on a $v_p(a_n) = v_p(a)$ et $v_p(b_n) = v_p(b)$ sont dans $\mathbf{N}$. On a alors $v_p(a_n b_n) \in \mathbf{N}$ et $v_p(a_n b_n) = v_p(a_n) + v_p(b_n)$. Pour un entier $n$ éventuellement encore plus grand, on a $v_p(ab) = v_p(a) + v_p(b) \in \mathbf{N}$ donc $ab$ n'est pas nul.

On en déduit que $\mathbf{Z}_p$ est intègre.

**36.** On vient de voir que, pour $a$ et $b$ non nuls dans $\mathbf{Z}_p$, on a $v_p(a \cdot b) = v_p(a) + v_p(b)$. Si $a - b$ est nul, on a bien $v_p(a + b) \geqslant min(v_p(a), v_p(b))$. On suppose $a$, $b$ et $a + b$ sont non nuls. Pour $n$ assez grand, on a $a_n + b_n$, $a_n$ et $b_n$ qui sont non nuls et $v_p(a_n + b_n) = v_p(a + b)$, $v_p(a) = v_p(a_n)$ et $v_p(b) = v_p(b_n)$. En utilisant les propriétés de la valuation dans $\mathbf{Z}$, on obtient alors $v_p(a - b) \geqslant \min(v_p(a), v_p(b))$.

**37.** $\theta(1)$ est la suite constante égale à 1 donc il s'agit de l'élément unité de l'anneau $\mathbf{Z}_p$. Soient $x$ et $y$

deux éléments de $\mathbf{Z}$. On pose $a = \theta(x)$, $b = \theta(y)$ et $c = \theta(x+y)$. Pour tout $n$, on a $a_n \equiv x[p^{n+1}]$ et $b_n \equiv y[p^{n+1}]$ ; on en déduit que $a_n + b_n \equiv x + y[p^{n+1}]$ et $a_n + b_n \equiv c_n[p^{n+1}]$. Comme, $c_n$ est entre 0 et $p^{n+1} - 1$ on a $c = a + b$, c'est-à-dire $\theta(x+y) = \theta(x) + \theta(y)$. On démontre de la même manière que $\theta(xy) = \theta(x)\theta(y)$.

Comme on a déjà montré que $\theta$ est injectif, on conclut que $\theta$ est un morphisme injectif d'anneaux.

**Q.38** Soit $a \in \mathbf{Z}_p$. Si $a$ est inversible, il existe $b \in \mathbf{Z}_p$ tel que, pour tout $n$, $a_n b_n \equiv 1[p^{n+1}]$. En particulier $a_0 b_0$ n'est pas nul donc $a_0$ non plus.

Réciproquement, supposons $a_0$ non nul. Pour $n \geqslant 1$, on a $a_n \equiv a_0[p]$, donc $a_n$ n'est pas divisible par $p$. On en déduit que $a_n$ est inversible modulo $p$. C'est le cas de $a_0$ donc il existe $b_0$ entre 0 et $p-1$ tel que $a_0 b_0 \equiv 1[p]$. Soit $n \geqslant 0$. On suppose avoir construit $b_0, \dots, b_n$ tel que, pour $k \leqslant n$, $a_k b_k \equiv 1[p^{k+1}]$ et $b_k \equiv b_{k-1}[p^k]$. On cherche alors $b_{n+1}$ de la forme $b_n + \beta p^{n+1}$ sachant que $a_{n+1}$ s'écrit $a_n + \alpha p^{n+1}$ et que $a_n b_n = 1 + \gamma p^{n+1}$ (avec $\alpha$, $\beta$ et $\gamma$ des entiers). On veut $a_{n+1} b_{n+1} \equiv 1[p^{n+2}]$ soit $a_n b_n + (a_n \beta + \alpha b_n) p^{n+1} + \alpha\beta p^{2n+2} \equiv 1[p^{n+2}]$. Ceci équivaut à dire que $p$ divise $\gamma + a_n\beta + b_n\alpha$. On peut choisir $\beta$ pour que ceci soit vrai puisque $a_n$ est inversible modulo $p$. Par récurrence sur $n$, on a alors construit $b = (b_n)_n \in \mathbf{Z}_p$ telle que $ab = \theta(1)$. L'élément $a$ est donc inversible dans $\mathbf{Z}_p$.

**Q.39** Si $\theta(p^k)$ divise $a$ dans $\mathbf{Z}_p$, il existe $b \in \mathbf{Z}_p$ tel que $a = \theta(p^k) \cdot b$. Pour $n \geqslant k$, on a $a_n \equiv p^k b_n [p^{n+1}]$ donc $v_p(a_n) \geqslant k$. On en déduit que $v_p(a) \geqslant k$.

Réciproquement, supposons que $v_p(a) \geqslant k$. Cela signifie que, pour $n < k$, on a $a_n = 0$ et pour $n \geqslant k$, $p^k$ divise $a_n$. On considère la suite $u$ comme dans la question **25.** telle que pour tout $n \in \mathbf{N}$, on a

$$a_n = \sum_{i=0}^{n} u_i p^i.$$

Pour $i < k$, on a $u_i = 0$ et pour $n \geqslant k$, $a_n = p^k \sum_{i=k}^{n} u_i p^{k-i}$. On définit alors l'élément $b = (b_n) \in \mathbf{Z}_p$ en posant pour tout $n \in \mathbf{N}$, $b_n = \sum_{i=0}^{n} u_{i+k} p^i$. Pour tout $n$, on a alors $p^k b_n \equiv a_n [p^{n+1}]$ donc $\theta(p^k) b = a$. On en déduit que $a$ est divisible par $\theta(p^k)$.

L'équivalence est démontré.

**40.** Soit $I$ un idéal de $\mathbf{Z}_p$, distinct de $\{0\}$. On note $A = \{v_p(a); a \in I \setminus \{0\}\}$. C'est une partie non vide de $\mathbf{N}$ qui admet donc un plus petit élément $k$ ; on peut alors considérer un élément $a \in I$ tel que $v_p(a) = k$. D'après la question précédente, on peut écrire $a = \theta(p^k) \cdot b$. On a $v_p(b) = 0$ donc $b$ est inversible et $\theta(p^k)$ est un multiple de $a$ ; ainsi $\theta(p^k) \in I$ et l'idéal engendré par $\theta(p^k)$ est inclus dans $I$.

Soit $b \in I \setminus \{0\}$, on a $v_p(b) \geqslant k$ donc $\theta(p^k)$ divise $b$. Par conséquent $I$ est inclus dans l'idéal engendré par $p^k$.

Par double inclusion, $I = \theta(p^k)\mathbf{Z}_p$ et les idéaux de $A$ sont les $p^k\mathbf{Z}_p$ pour $k \in \mathbf{N}$ et $\{0\}$.

**41.** Si $\dfrac{a}{b} = \dfrac{c}{d}$, alors $ad = bc$ donc, comme $\theta$ est un morphisme d'anneaux, $\theta(a)\theta(d) = \theta(b)\theta(c)$ et les classes de $(\theta(a), \theta(b))$ et $(\theta(c), \theta(d))$ sont égales. L'application est donc bien définie.

On démontre que c'est un morphisme d'anneaux (en utilisant que $\theta$ en est un).

Si les classes de $(\theta(a), \theta(b))$ et $(\theta(c), \theta(d))$ sont égales, on a $\theta(a)\theta(d) = \theta(c)\theta(b)$ et, comme $\theta$ est un morphisme injectif, $ad = bc$. Il s'agit donc d'un morphisme injectif.

**42.** Si $ad = bc$, alors en utilisant la question **36.**, on a $v_p(a) + v_p(d) = v_p(b) + v_p(c)$ donc $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

**43.** Si $x \in \mathbf{Z}_p$, alors $x$ est la classe de $(a, 1)$ avec $a \in \mathbf{Z}_p$. On a alors $v_p(x) = v_p(a) \geqslant 0$.

Réciproquement, supposons que $v_p(x) \geqslant 0$; alors $x$ est la classe de $(a, b)$ avec $v_p(a) \geqslant v_p(b)$. On pose $a = \theta(p^k)a'$ et $b = \theta(p^l)b'$ avec $v_p(a') = v_p(b') = 0$ et $k \geqslant l$ et $x$ est la classe de $(\theta(p^{k-l})a', b')$. Puisque $v_p(b') = 0$ on en déduit que $b'$ est inversible dans $\mathbf{Z}_p$. Si $c'$ est son inverse dans $\mathbf{Z}_p$, alors $x$ est la classe de $(p^{k-l}a'c', 1)$ qui est dans $\mathbf{Z}_p$.

On a démontré l'équivalence.

## II.C Topologie dans $\mathbf{Q}_p$

**44.** Pour $k > n$, on a $a_k - a_n = \sum_{i=n+1}^{k} u_i p^i$ donc $v_p(a_k - a_n) \geqslant n+1$ et, par conséquent, on a $v_p(a - \theta(a_n)) \geqslant n+1$ et $|a - \theta(a_n)|_p \leqslant \dfrac{1}{p^{n+1}}$. On peut alors conclure que la suite $(\theta(a_n))$ converge vers $a$ dans $\mathbf{Z}_p$.

**45.** La question précédente montre que tout élément de $\mathbf{Z}_p$ est la limite d'une suite d'éléments de $\theta(\mathbf{Z})$ donc $\theta(\mathbf{Z})$ est dense dans $\mathbf{Z}_p$.

**46.** Soit $a$ la suite $(a_n)$ avec, pour tout $n$, $a_n = \sum_{i=0}^{n} u_i p^i$. Si, pour $i < l$, on a $u_i = 0$ ; alors pour $n \geqslant l$, on a $a_n = \sum_{i=l}^{n} u_i p^i$ et $v_p(a_n) \geqslant l$. On en déduit $v_p(a) \geqslant l$.

Réciproquement, si $v_p(a) \geqslant l$, alors pour $n$ assez grand, on a $v_p(a_n) \geqslant l$ et $p^l$ divise $\sum_{i=0}^{n} u_i p^i$. Par conséquent, $p^l$ divise $p^i$ pour $i \geqslant l$ donc $p^l$ divise $\sum_{i=0}^{l-1} u_i p^i$. Ceci n'est possible que si $u_0 = \cdots = u_{l-1} = 0$.

On en déduit l'équivalence.

**47.** a) Soit $i \in \mathbf{N}$. Comme la suite $(a^{(k)})$ est de Cauchy, on a $\lim_{k \to +\infty} |a^{(k)} - a^{(k+1)}|_p = 0$ et, pour $k$ assez grand, $v_p(a^{(k)} - a^{(k+1)}) \geqslant i+1$. Comme dans la question précédente, on en déduit que $u_i^{(k)} = u_i^{(k+1)}$ donc la suite $(u_i^{(k)})_k$ est stationnaire.

b) Pour tout $i \in \mathbf{N}$, on note $v_i$ l'entier tel que, pour $k$ assez grand, $u_i^{(k)} = v_i$. Soit $x = \sum_{i=0}^{+\infty} v_i p^i$. Soit $n \in \mathbf{N}$. Pour $k$ assez grand, pour tout $i \leqslant n$, $u_i^{(k)} = v_i$. On a alors $v_p(x - a^{(k)}) \geqslant n$ et $|x - a^{(k)}|_p \leqslant p^{-n}$. Ceci permet de conclure que $(a^k)$ converge vers $x$.
Par conséquent, $\mathbf{Z}_p$ est complet.

**48.** Si la suite $(S_n)$ converge, alors $(S_n - S_{n-1})_n$ converge vers 0 donc $(x_n)$ converge vers 0.
Réciproquement, supposons que $(x_n)$ converge vers 0. Pour $n$ et $l$ deux entiers naturels, $S_{n+l} - S_n = \sum_{k=n+1}^{n+l} x_k$. D'après l'inégalité vérifiée par la valeur absolue $p$-adique, on a $|S_{n+l} - S_n|_p \leqslant \max_{n+1 \leqslant k \leqslant n+l} |x_k|_p$.
Soit $\varepsilon > 0$ et $n_\varepsilon \in \mathbf{N}$ tel que, si $k \geqslant n_\varepsilon$, $|x_k|_p \leqslant \varepsilon$. Alors, pour $n \geqslant n_\varepsilon$ et $l \in \mathbf{N}$, $|S_{n+l} - S_n|_p \leqslant \varepsilon$. Par conséquent, $(S_n)$ est une suite de Cauchy de $\mathbf{Q}_p$, qui est complet, donc elle converge.

## Partie III : Termes nuls d'une suite récurrente linéaire

**49.** On pose $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & \cdots & \cdots & \cdots & a_{d-1} \end{pmatrix}$.

On a alors, pour tout $n \in \mathbf{N}$, $U_{n+1} = AU_n$ et, par récurrence, $U_n = A^n U_0$. Avec $X = (1, 0, \ldots, 0)^T$, on a $u_n = X^T U_n = X^T A^n U_0$.

**50.** En développant par rapport à la première colonne, $\det(A) = (-1)^{d+1} a_0 \det(I_{d-1}) \neq 0$ donc $A$ est

inversible.

**51.** Soit $p$ un nombre premier impair qui ne divise pas $a_0$ (il suffit de choisir $p > |a_0|$). Alors $p$ ne divise pas $\det(A)$. Par ailleurs, $\overline{\det(A)} = \det(\overline{A})$ (par exemple en exprimant le déterminant comme une somme sur le groupe symétrique $\mathcal{S}_n$) donc pour un tel $p$, $\det(\overline{A})$ n'est pas nul dans $\mathbf{Z}/p\mathbf{Z}$ et $\overline{A} \in GL_d(\mathbf{Z}/p\mathbf{Z})$.

**52.** $GL_d(\mathbf{Z}/p\mathbf{Z})$ est un groupe de cardinal fini donc tous ses éléments sont d'ordre fini. Il existe donc un entier $k$ tel que $\overline{A}^k = I_d$ (dans $GL_d(\mathbf{Z}/p\mathbf{Z})$). Cela signifie que tous les coefficients de $A^k - I_d$ sont divisibles par $p$ : il existe $B \in \mathcal{M}_d(\mathbf{Z})$ telle que $A^k = I_d + pB$.

**53.** Soient $n$ et $j$ deux entiers naturels.

$$v_p(p^j f_j(n)/j!) = j - v_p(j!) + v_p(f_j(n)).$$

$f_j(n) \in \mathbf{Z}$ donc $v_p(f_j(n)) \geqslant 0$. De plus, $v_p(j!) \leqslant \dfrac{j}{p-1}$ donc $v_p(p^j f_j(n)/j!) \geqslant 0$. On en déduit que $p^j \dfrac{f_j(n)}{j!} \in \mathbf{Z}_p$.

**54.** En reprenant le calcul précédent et en remarquant que $\dfrac{1}{p-1} < 1$, on obtient que $\lim\limits_{j\to+\infty} v_p(p^j f_j(n)/j!) = +\infty$ et donc $\lim\limits_{j\to+\infty} |v_p(p^j f_j(n)/j!)|_p = 0$. Avec la fin de la partie II, cela permet de conclure que la série $\sum\limits_j v_p(p^j f_j(n)/j!)$ converge dans $\mathbf{Q}_p$. Il s'agit d'une suite de $\mathbf{Z}_p$ qui est fermé (car complet) donc la limite est dans $\mathbf{Z}_p$.

**55.** On a, pour $n \in \mathbf{N}$, $u_{kn+r} = X^T(I + pB)^n A^r U_0$. $I$ et $B$ commutent donc on peut utiliser la formule du binôme :

$$u_{kn+r} = \sum_{j=0}^{n} p^j f_j(n)/j!$$

où $f_j(n) = X^T B^j A^r U_0 n(n-1)\cdots(n-j+1)$. Pour $j > n$, $f_j(n) = 0$ donc on peut écrire

$$u_{kn+r} = \sum_{j=0}^{+\infty} p^j f_j(n)/j!.$$

Le résultat admis permet alors de conclure.

# Partie IV : exponentielle $p$-adique et application

## IV.A Définition de l'exponentielle

**56.** Pour $n \geqslant 1$ et $x \in \mathbf{Q}_p$, on pose $u_n(x) = \dfrac{x^n}{n!}$.Alors $v_p(u_n(x)) = nv_p(x) - v_p(n!)$. D'après la partie I.B, $v_p(n!) \leqslant \dfrac{n}{p-1}$ donc $v_p(u_n(x)) \geqslant n\left(v_p(x) - \dfrac{1}{p-1}\right)$. Or, par hypothèse, $v_p(x) > \dfrac{1}{p-1}$ donc $\lim\limits_{n\to+\infty} v_p(u_n(x)) = +\infty$ et $\lim\limits_{n\to+\infty} |u_n(x)|_p = 0$. La fin de la partie II permet alors de conclure que la série $\sum \dfrac{x^n}{n!}$ converge.

**57.** Soient $x$ et $y$ dans $\mathbf{Q}_p$ tels que $v_p(x)$ et $v_p(y)$ soient strictement supérieurs à $\dfrac{1}{p-1}$. Comme $v_p(x+y) \geqslant \min(v_p(x), v_p(y))$, on a $v_p(x+y) > \dfrac{1}{p-1}$. La question précédente montre alors que

$e_p(x+y)$ est défini.

Soient $N \in \mathbf{N}$, $I_N = \{(k,l) \in [\![0;N]\!]^2 \;/\; N < k+l\}$ et $\Delta_N = \sum_{(k,l)\in I_N} \frac{x^k y^l}{k!l!}$. En utilisant la formule du binôme de Newton (dans l'anneau commutatif $(\mathbf{Q}_p, +, \cdot)$),

$$\left(\sum_{k=0}^{N} \frac{x^k}{k!}\right)\left(\sum_{l=0}^{N} \frac{y^l}{l!}\right) - \sum_{n=0}^{N} \frac{(x+y)^n}{n!} = \Delta_N.$$

Pour conclure, il suffit donc de démontrer que $(\Delta_N)$ tend vers 0. D'après l'inégalité triangulaire, $|\Delta_N|_p \leqslant \sum_{(k,l)\in I_N} |x^k/k!|_p |y^l/l!|_p$. Comme dans la question précédente, $v_p(x^k/k!) \geqslant k(v_p(x) - 1/(p-1))$ donc, si on pose $\alpha_1 = 1/p^{v_p(x)-1/(p-1)}$ et $\beta_1 = 1/p^{v_p(y)-1/(p-1)}$, $0 \leqslant \alpha_1 < 1$, $0 \leqslant \beta_1 < 1$ et $|\Delta_n|_p \leqslant \sum_{(k,l)\in I_N} \alpha_1^k \beta_1^l$. Les séries $\sum \alpha_1^k$ et $\sum \beta_1^l$ convergent absolument dans $\mathbf{R}$ donc on peut en faire le produit de Cauchy qui permet de montrer que $\lim_{N\to+\infty} \sum_{(k,l)\in I_N} \alpha_1^k \beta_1^l = 0$. Par le théorème d'encadrement (dans $\mathbf{R}$), $\lim_{N\to+\infty} |\Delta_N|_p = 0$ ce qui signifie que $\lim_{N\to+\infty} \Delta_N = 0$ (dans $\mathbf{Q}_p$). Puisqu'il est admis que les opérations algébriques sur les limites sont licites, on obtient en passant à la limite : $e_p(x+y) = e_p(x)e_p(y)$.

**58.** Soit $t$ tel que $|t|_p < 1$. On a alors $v_p(t) \geqslant 1$. Pour $n \in \mathbf{N}^*$, $v_p((-1)^{n+1}t^n/n) = nv_p(t) - v_p(n) \geqslant n - v_p(n)$. Comme $n \geqslant p^{v_p(n)}$, $v_p(n) = O(\ln(n))$ et $\lim_{n\to+\infty} (n - v_p(n)) = +\infty$ et $\lim_{n\to+\infty} |(-1)^{n+1}t^n/n|_p = 0$. En utilisant la partie II, on en déduit que $\sum (-1)^{n+1}\frac{t^n}{n}$ converge.

# IV.B. Inversibles de $(\mathbf{Z}/n\mathbf{Z})^*$.

**59.** On a vu dans l'exercice 2, question 5 que $(\mathbf{Z}/p^n\mathbf{Z})^*$ est de cardinal $p^n - p^{n-1}$.

**60.** Soit $u = \overline{a} \in \mathbf{Z}/p^n\mathbf{Z}$. $1 + pu$ n'est pas divisible par $p$ donc est premier avec $p^n$. Par conséquent, $\overline{1} + pu$ est inversible dans $\mathbf{Z}/p^n\mathbf{Z}$. Ainsi, $\overline{1} + p\mathbf{Z}/p^n\mathbf{Z}$ est inclus dans $(\mathbf{Z}/p^n\mathbf{Z})^*$ ; il contient $\overline{1}$ donc il est non vide.
Soient $u$ et $v$ deux éléments de $\mathbf{Z}/p^n\mathbf{Z}$. Alors $(\overline{1}+pu)(\overline{1}+pv) = \overline{1} + p(u+v+puv)$ avec $u+v+puv \in \mathbf{Z}/p^n\mathbf{Z}$. Donc $\overline{1}+pv$ est l'inverse de $\overline{1}+pu$ si et seulement si $p(u+v+puv) = \overline{0}$. Pour cela, il suffit d'avoir $(\overline{1}+pu)v = -u$. Soit $w$ l'inverse de $\overline{1}+pu$ dans $\mathbf{Z}/p^n\mathbf{Z}$. On pose alors $v = -wu$. D'après ce qui précède, l'inverse de $\overline{1}+pu$ est $\overline{1}+pv \in \overline{1} + p\mathbf{Z}/p^n\mathbf{Z}$.
On peut alors conclure que $(1 + p\mathbf{Z}/p^n\mathbf{Z}, \times)$ est un sous groupe de $(\mathbf{Z}/p^n\mathbf{Z})^*$.

**61.** **(a)** Soit $x \in \mathbf{Z}$ tel que $\tilde{x}$ engendre $(\mathbf{Z}/p\mathbf{Z})^*$. Comme $x$ est premier avec $p$, il l'est avec $p^n$ et $\overline{x}$ est dans $(\mathbf{Z}/p^n\mathbf{Z})^*$. On note $r$ l'ordre de $\overline{x}$ (dans $(\mathbf{Z}/p^n\mathbf{Z})^*$). Comme $\pi$ est un morphisme, $\tilde{x}^r = \tilde{1}$ et $r$ est un multiple de $p-1$. Soit $k$ tel que $r = k(p-1)$ ; d'après le théorème de Lagrange, $r$ divise $p^{n-1}(p-1)$ donc $k$ divise $p^{n-1}$ et est donc premier avec $p-1$. On pose alors $a = x^k$. On a alors que $\tilde{a} = \tilde{x}^k$ engendre $(\mathbf{Z}/p\mathbf{Z})^*$ (car ce groupe est cyclique de cardinal premier avec $k$). De plus $\overline{a}$ est bien d'ordre $p-1$.

**(b)** On considère un entier $a$ comme dans la question précédente.
Pour deux entiers $i$ et $j$, si $\tilde{a}^i = \tilde{a}^j$, cela signifie que $i \equiv j[p-1]$ et, comme $\overline{a}$ est d'ordre $p-1$, $\overline{a}^i = \overline{a}^j$. On peut donc définir une application $\varphi$ de $(\mathbf{Z}/p\mathbf{Z})^*$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$ en posant, pour $i \in \mathbf{N}$, $\varphi(\tilde{a}^i) = \overline{a}^i$. Il est alors immédiat que $\varphi$ est bien un morphisme et qu'il vérifie $\pi \circ \varphi = id$.

**(c)** En gardant les notations de la question précédente, on considère l'application $\psi$ définie sur $\left(\overline{1} + p\mathbf{Z}/p^n\mathbf{Z}\right) \times (\mathbf{Z}/pZ)^*$ par $\psi(\overline{1}+pu, v) = (\overline{1}+pu)\varphi(v)$. Cett application est un morphisme de groupes.
Si $\psi(\overline{1}+pu, v) = \overline{1}$, en appliquant $\pi$, on obtient $v = \tilde{1}$ (car $\pi \circ \varphi$ est l'identité) puis $\varphi(v) = \overline{1}$ et

enfin $\overline{1} + pu = \overline{1}$. On en déduit que $\psi$ est injectif.
Par ailleurs, les groupes $\left(\overline{1} + p\mathbf{Z}/p^n\mathbf{Z}\right) \times (\mathbf{Z}/pZ)^*$ et $(\mathbf{Z}/p^n\mathbf{Z})^*$ ont le même cardinal $p^{n-1}(p-1) = p^n - p^{n-1}$ donc $\psi$ est un isomorphisme.

**62.** Soit $x \in p\mathbf{Z}_p$. Alors $v_p(x) \geqslant 1 > \dfrac{1}{p-1}$ donc $e_p(x)$ existe. De plus, pour $n \in \mathbf{N}$, $v_p(x^n/n!) = nv_p(x) - v_p(n!) > 0$ donc $x^n/n! \in \mathbf{Z}_p$. La série $\sum \dfrac{x^n}{n!}$ converge dans $\mathbf{Q}_p$, est à termes dans $\mathbf{Z}_p$ qui est fermé donc sa somme appartient à $\mathbf{Z}_p$. On en déduit que $e_p(x) \in \mathbf{Z}_p$.

**63.** Soient $x$ et $x'$ deux représentants de $X$. Puisque $x$ est un entier relatif donc $v_p(x) \in \mathbf{N}$ et $v_p(x) > \dfrac{1}{p-1}$, $e_p(x)$ est bien défini. Si $x' = x + p^n i$ avec $i \in \mathbf{Z}$ alors $e_p(x') = e_p(x)e_p(p^n i)$. Pour tout entier $k$, $v_p\left(\dfrac{(p^n i)^k}{k!}\right) = kn + kv_p(i) - v_p(k!) \geqslant kn \geqslant n$. On en déduit que $e_p(p^n i) \geqslant n$ et donc $p^n$ divise $e_p(p^n i)$. Ainsi, il existe $y \in \mathbf{Z}_p$ tel que $e_p(x') = e_p(x)(1 + p^n y)$. On en déduit que $\pi_n(e_p(x)) = \pi_n(e_p(x'))$.

**64.** D'après ce qui précède, $E_p$ est un morphisme de $(p\mathbf{Z}/p^n\mathbf{Z}, +)$ dans $(1 + p\mathbf{Z}/p^n\mathbf{Z}, \times)$. Comme $L_P$ est son application réciproque, c'est un isomorphisme (on définit $L_p$ à partir de $l_p$ en suivant la même méthode que pour $E_p$ à partir de $e_p$).

**65.** La classe de 5 engendre $(5\mathbf{Z}/125\mathbf{Z}, +)$ donc $E_p(5)$ engendre $(1 + 5\mathbf{Z}/125\mathbf{Z}, \times)$. On calcule l'exponentielle 5-adique de 5 en réduisant modulo $125 = 5^3$.De plus, $v_5(5^n/n!) = n - v_5(n!) \geqslant n(1 - 1/4)$ donc $v_5(5^n/n!) \geqslant 3n/4$. Pour $n \geqslant 4$, $v_5(5^n/n!) \geqslant 3$. Par conséquent, en calculant modulo 125,

$$\exp(5) = 1 + 5 + \frac{5^2}{2} + \frac{5^3}{3!} = 6 + 12 + \frac{1}{2} + 21 - \frac{1}{6} = 39 + \frac{1}{3}$$

De plus, $42 \times 3 = 126$ et $42 = 2 + 3 \times 5 + 5^2$ donc, modulo 125, $\dfrac{1}{3} = 42$.
Ainsi la classe de 81 engendre $(1 + 5\mathbf{Z}/125\mathbf{Z}, +)$.

**66.** D'après ce qui précède, $(\mathbf{Z}/p^n\mathbf{Z})^*$ est isomorphe à $((\mathbf{Z}/p\mathbf{Z})^*, \cdot) \times ((p\mathbf{Z}/p^n\mathbf{Z}), +)$. Il s'agit du produit de deux groupes cycliques d'ordres premiers entre eux donc, d'après le lemme chinois, $((\mathbf{Z}/p^n\mathbf{Z})^*, \cdot)$ est un groupe cyclique.